HONORABLE RICARDO S. MARTINEZ

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

In re MCG Health Data Security Issue Litigation	Case No. 2:22-cv-00849-RSM-DWC **FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Diana Saiki, Kenneth Hensley, as legal guardian of R.H., Linda Crawford, Julie Mack, Linda Booth, Candace Daugherty, Leo Thorbecke, Cynthia Strecker, Michael Price, Blanca Garcia, Joanne Mullins, Marjorita Dean, Kelly Batt, Jay Taylor, Shelley Taylor, and Gaye Ictech ("Plaintiffs") individually and on behalf of all others similarly situated, and by and through their undersigned counsel file this Consolidated Class Action Complaint against Defendant MCG Health, LLC ("MCG" or "Defendant") and allege the following based upon personal knowledge of the facts, and upon information and belief based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. Defendant MCG Health is a healthcare consulting company that provides patient care guidelines and health plans that include care strategies, analytics, software solutions, and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

other services to hospitals, government programs, and health plans across the country. In this role, Defendant operates as a covered business associate as defined by the Health Insurance Portability and Accountability Act ("HIPAA") and is required to comply with HIPAA regulations. *See* 45 CFR 160.103.

2. As a condition of receiving services, MCG's client's and their patients are required to provide and entrust MCG with sensitive and private information, including personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information"). The PII and PHI that Defendant collects and maintains includes, but is not limited to, patient names, genders, telephone numbers, addresses, email addresses, dates of birth, Social Security numbers, and medical code information.

3. On June 10, 2022, MCG publicly disclosed that on March 25, 2022, it detected that an unauthorized individual had obtained Private Information stored on MCG's computer network pertaining to approximately 1,100,000 persons (the "Data Breach"). Roughly two and half months after discovering that criminals had obtained the Private Information of over a million victims of the Data Breach, MCG began sending notice letters to States Attorneys General, Plaintiffs, and Class Members (the "Notice").

4. MCG's Notice provided scant detail, particularly considering the size and scope of the Data Breach and the sensitivity of Plaintiffs' and Class Members' compromised information. MCG's Notice stated, in relevant part, "that an unauthorized party previously obtained certain of your personal information that matched data stored on MCG's systems," that MCG "took steps to understand [the Data Breach's] nature and scope," and that MCG had "deployed additional monitoring tools and will continue to enhance the security of our systems."

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

5. MCG's Notice did not disclose when the Data Breach began or how long criminals had access to its systems, the means and mechanism of the cyberattack, the reason for the two-and-a-half month delay in notifying Plaintiffs and the Class of the Data Breach, how MCG determined that the Private Information had been "obtained," and, importantly, what steps MCG took following the Data Breach to secure its systems and prevent further cyberattacks.

6. MCG informed the Maine Attorney General that "the data may have been acquired by an unauthorized party on or around February 25-26, 2020" but "there is uncertainty regarding the date the breach occurred."[1] That the Data Breach went undetected for over two years by a sophisticated provider of data management services and software solutions to the healthcare industry makes Defendant's security failure all the more egregious.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' and employees' Private Information from the foreseeable threat of a cyberattack.

8. By taking possession and control of Plaintiffs' and Class Members' Private Information for its own pecuniary benefit, Defendant assumed a duty to securely store and protect the Private Information in its custody from the risk of a cyber intrusion. Defendant also had a duty to adequately safeguard this Private Information under industry standards and duties imposed by statutes, including HIPAA regulations and Section 5 of the Federal Trade Commission Act ("FTA Act").

9. As a result of MCG's failure to implement adequate data security practices, Plaintiffs and over a million Class Members suffered injury and ascertainable losses in the form

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/1948d82a-0cdb-4b37-a988-b4189351176b.shtml

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from its exposure, and the present and imminent threat of fraud and identity theft.

10. The injury to Plaintiffs and Class Members was compounded by the fact that Defendant did not notify patients that their Private Information was subject to unauthorized access and exfiltration until June 10, 2022, nearly two-and-a-half months after the Data Breach was discovered. Defendant's failure to timely notify the victims of its Data Breach meant that Plaintiffs and Class Members were unable to take affirmative measures to prevent or mitigate the resulting harm.

11. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiffs' and Class Members' sensitive and confidential Private Information still remains in the possession of Defendant. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

12. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiffs and Class Members prompt and adequate notice of the Data Breach.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

13. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether.

14. The security of Plaintiffs' and Class Members' identities is now at risk because of Defendant's wrongful conduct as the Private Information that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their course of their lives.

15. Armed with the Private Information accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in their names, using Class Members' identities to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's licenses in Class Members' names, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts and medical records to guard against identity theft. Further, Plaintiffs and Class Members will incur out-of-pocket costs to purchase credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Plaintiffs and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts and medical records for fraud or identity theft. And because the exposed information includes their Social Security numbers and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

18. Through this action, Plaintiffs and Class Members seek to hold Defendant responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiffs seek to remedy the harms resulting from the Data Breach on behalf of themselves and all similarly situated individuals whose Private Information was accessed and exfiltrated during the Data Breach.

19. Plaintiffs and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorney's fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

II. THE PARTIES

20. Plaintiff Diana Saiki is a resident and citizen of the State of Indiana.

21. Plaintiff Leo Thorbecke is a resident and citizen of the State of Indiana.

22. Plaintiff Kenneth Hensley, as legal guardian of R.H., is a resident and citizen of the State of Indiana.

23. Plaintiff Michael Price is a resident and citizen of the State of Illinois.

24. Plaintiff Linda Crawford is a resident and citizen of the State of Kansas.

25. Plaintiff Kelly Batt is a resident and citizen of the State of California.

26. Plaintiff Shelley Taylor is a resident and citizen of the State of Kentucky.

27. Plaintiff Jay Taylor is a resident and citizen of the State of Kentucky.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

28. Plaintiff Gaye Ictech is a resident and citizen of the State of Louisiana.

29. Plaintiff Cynthia Strecker is a resident and citizen of the State of Louisiana.

30. Plaintiff Candace Daugherty is a resident and citizen of the State of Mississippi.

31. Plaintiff Linda Booth is a resident and citizen of the State of New Mexico.

32. Plaintiff Blanca Garcia is a resident and citizen of the State of New Mexico.

33. Plaintiff Marjorita Dean is a resident and citizen of the State of Ohio.

34. Plaintiff Julie Mack is a resident and citizen of the State of Texas.

35. Plaintiff Joanne Mullins is a resident and citizen of the State of Texas.

36. Defendant MCG Health is a Washington limited liability company with its principal place of business at 901 Fifth Avenue, Suite 120, Seattle, WA 98164.

III. JURISDICTION AND VENUE

37. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant.

38. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District and Defendant conducts substantial business in Washington and this District through its headquarters and offices; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

39. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant's principal place of business is in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant is a HIPAA covered business associate.

40. Defendant is a HIPAA covered business associate that provides software and other services to various health care providers and health plans (i.e., HIPAA "Covered Entities"). As a regular and necessary part of its business collects and custodies the highly sensitive Private Information of its clients' patients and health plan members. Defendant is required under federal and state law to maintain the strictest confidentiality of the patient's and plan members' Private Information that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

41. As a HIPAA covered business entity, Defendant is required to enter into contracts with its Covered Entities to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule[2] and to report to the Covered Entities any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

[2] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

42. As a condition of receiving Defendant's services, Defendant requires that Covered Entities and their patients and plan members, including Plaintiffs and Class Members, entrust it with highly sensitive personal information. Due to the nature of Defendant's business, which includes providing patient care guidelines, health plans, consulting, analytics, and software solutions, Defendant would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

B. The Data Breach compromised Private Information.

43. On March 25, 2022, according to the Notice MCG provided to Plaintiffs and Class Members, MCG determined that cybercriminals had gained unauthorized access to its systems and "*obtained*" confidential personal information about patients and plan members whose Private Information was stored on Defendant's systems. As reflected by Defendant's disclosure of the Data Breach to the Maine Attorney General, Defendant was unable to determine when its systems were actually compromised as Defendant acknowledged that "the data may have been acquired by an unauthorized party on or around February 25-26, 2020" but "there is uncertainty regarding the date the breach occurred." Defendant's lack of adequate data security practices is evidenced by the fact that Defendant did not discover that its systems were compromised for two years following the Data Breach.

44. In the letter sent to Plaintiffs and Class Members, two years after its systems were compromised and two and a half months following its discovery of the Data Breach, Defendant finally acknowledged, in a roundabout way, that:

> an unauthorized party previously obtained certain of your personal information that matched data stored on [MCG's] systems. The affected patient or member data

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> included some or all of the following data elements: names, Social Security numbers, medical codes,[3] postal addresses, telephone numbers, email addresses, dates of birth, and gender.[4]

45. Defendant's Notice letter also vaguely describes the measures it took following its belated discovery of the Data Breach stating only that:

> Upon learning of this issue, we took steps to understand its nature and scope. A leading forensic investigation firm was retained to assist in the investigation. Additionally, we are coordinating with the FBI. We have deployed additional monitoring tools and will continue to enhance the security of our systems.

46. Tellingly, Defendant's Notice omits that fact that it was unable to determine when its systems were first breached but that it believes the Data Breach to have occurred two years earlier, on or about February 25 or 26 of 2020.

47. Defendant's Notice omits pertinent information including how long criminals had access to its systems, the means and mechanism of the cyberattack, the reason for the two and a half month delay in noticing Plaintiffs and Class Members of the Data Breach, how it determined that the Private Information had been "obtained," why it us unable to determine when its systems were first compromised, and of particular importance to Plaintiffs and Class Members, what actual steps MCG took following the Data Breach to secure its systems and prevent further cyberattacks.

48. Based on Defendant's acknowledgement that the Private Information that it collected was "obtained" by cybercriminals, it is evident that unauthorized criminal actors did in fact access Defendant's network and exfiltrate Plaintiffs' and Class Members' Private

---

[3] Medical codes are alphanumeric designators used to document patient diagnoses, treatments, services, and supplies provided to the patient and circumstances or medical conditions relevant to treatments and services the patient receives.

[4] https://www.mcg.com/wp-content/uploads/2022/06/MCG-Website-Notice_90273447_1-6.8.22481312.4-004.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Information in an attack designed to acquire that sensitive, confidential, and valuable information.

49. The Private Information contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have "obtained" Plaintiffs and Class Members Private Information.

50. As a HIPAA associated business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Defendant was aware and knew it had a duty to guard against.

51. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and/or plan members, like Plaintiffs and Class Members.

52. Despite failing to detect the Data Breach for more than two years after Defendant's systems were compromised, Defendant waited more than two months following the completion of its investigation to notify the impacted individuals of the Data Breach and of the need for them to protect themselves against fraud and identity theft. Defendant was, of course, too late in the discovery and notification of the Data Breach.

53. Due to Defendant's inadequate security measures and its delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

54. Defendant had obligations created by HIPAA, contract, industry standards and common law made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

55. Plaintiffs and Class Members entrusted their Private Information to Defendant's clients with the reasonable expectation and mutual understanding that Defendant or anyone who used their Private Information in conjunction with the healthcare services they received would comply with obligations to keep such information confidential and secure from unauthorized access after it received such information.

56. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

57. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiffs and Class Members would not have allowed Defendant or anyone in Defendant's position to receive their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

58. As a result of Defendant's negligent and wrongful conduct, Plaintiffs' and Class Members' highly confidential and sensitive Private Information was left exposed to cybercriminals.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

C. Defendant was obliged under HIPAA to safeguard the Private Information.

59. Defendant is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

60. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

61. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

62. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

63. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

64. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

65. HIPAA's Security Rule requires Defendant to do the following:

[5] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

66. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

67. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

68. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[6]

69. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

70. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

71. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[7] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard

[6] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).
[7] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[8]

D. Defendant failed to follow FTC guidelines.

72. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

73. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

74. According to the FTC, the need for data security should be factored into all business decision-making.

75. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

76. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

77. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating

[8] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

78. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. Defendant failed to properly implement basic data security practices.

81. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' and plan members Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

82. Defendant was at all times fully aware of its obligation to protect the Private Information of the patients and plan members about whom it stored Private Information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

E. Defendant failed to comply with industry standards.

83. As described above, experts studying cyber security routinely identify healthcare providers and their business associates as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

84. Several best practices have been identified that at a minimum should be implemented by HIPAA covered business entities like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

85. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

86. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

87. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

F. Defendant owed Plaintiffs and Class Members a duty to safeguard their Private Information.

88. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

89. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

90. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

91. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

92. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

93. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

G. The Data Breach and its consequences were readily foreseeable risks to MCG.

94. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

95. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[9] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[10] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[11]

96. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April

[9] *See 2021 Data Breach Annual Report* (ITRC, Jan. 2022), available at https://notified.idtheftcenter.org/s/, at 6.
[10] *Id.*
[11] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

97. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[12]

98. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[13]

99. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[14]

100. Defendant was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were

[12] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.
[13] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360. arn-of-targeted-ransomware (last visited July 2, 2021).
[14] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[15]

101. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[16]

102. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

103. Defendant was on notice that the federal government has been concerned about healthcare company data encryption practices. Defendant knew its employees accessed and utilized protected health information in the regular course of their duties, yet it appears that information was not encrypted.

104. The OCR urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal

---

[15] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[16] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

information. In announcing the fines, Susan McAndrew, OCR's deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[17]

105. As a HIPAA covered business associate, Defendant should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

H. Data Breaches place Consumers at an immediate risk of fraud and identity theft.

106. Plaintiffs' and Class Members' Private Information is of great value to cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used by criminals to exploit Plaintiffs and the Class Members and to profit off the Private Information stolen from Defendant in the Data Breach.

107. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[18] For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other

[17] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[18] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

harmful forms of identity theft.[19] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

108. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web black-markets for years.[20]

109. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.[21]

110. The Private Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[22]

111. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

---

[19] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[21] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

[22] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[23] *Data Breaches Are Frequent*, *supra* note 11.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

112. For instance, with a stolen Social Security number, which is only one subset of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[24]

113. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

114. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

115. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

[24] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

116. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account.[25] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[26]

117. Identity thieves can use the Private Information stolen from Plaintiffs and Class Members to qualify for expensive medical care and leave them and their health insurers on the hook for massive medical bills. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[27] "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[28]

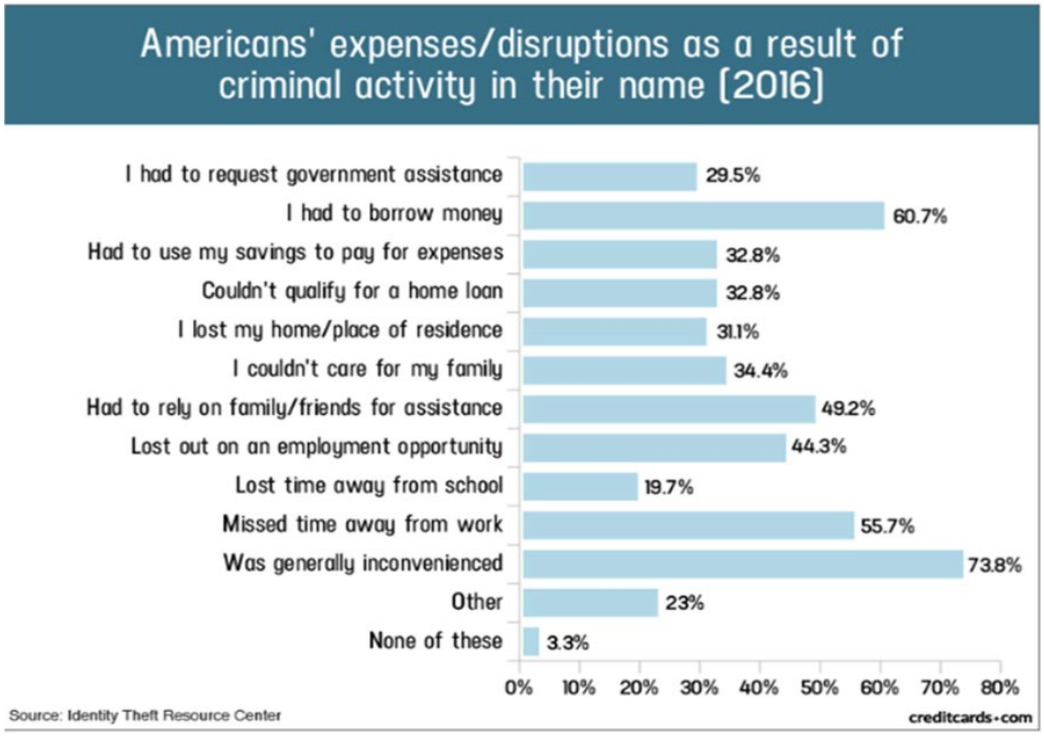
118. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law

[25] See Omri Toppol, Email Security: How You Are Doing It Wrong & Paying Too Much, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/
[26] *See* Vaas, Cyberattacks, *supra*, n. 28.
[27] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/
[28] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

119. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.[29]



120. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[30]

121. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud

[29] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.
[30] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and identity theft. Plaintiffs and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

122. Plaintiffs and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including Private Information;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Private Information being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

123. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' Private Information.

124. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Defendant knew or should have known about these dangers and strengthened its data security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

I. The Data Breach was foreseeable and preventable.

125. Data disclosures and data breaches are preventable.[31] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that

[31] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[32] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[33]

126. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[34]

127. Plaintiffs and Class Members entrusted their Private Information to Defendant as a condition of receiving healthcare related services from Defendant's clients. Plaintiffs and Class Members understood and expected that Defendant or anyone in Defendant's position would safeguard their PII and PHI against cyberattacks, delete or destroy Private Information that Defendant was no longer required to maintain, and timely and accurately notify them if their Private Information was compromised.

J. Plaintiffs' and Class Members damages.

128. To date, Defendant has done nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has merely offered Plaintiffs and Class Members identity protection and credit monitoring services for two years, but this service does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. Moreover, following the expiration of the two-year

[32] *Id.* at 17.
[33] *Id.* at 28.
[34] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

subscription, Plaintiffs and Class Members will be required to pay for credit monitoring services out of their own pocket which they will require as the threat of identity theft and fraud does not extinguish after a two-year period but persists for the remainder of Plaintiffs' and Class Members' lives.

129. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

130. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

131. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

132. Plaintiffs and Class Members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

133. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

134. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Private Information, a form of property that MCG obtained from Plaintiffs and Class Members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

135. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

136. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

137. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online, is properly encrypted, and that access to such data is password protected.

138. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiff's and Class Members' Private Information.

139. Defendant maintained the Private Information in an objectively reckless manner, making the Private Information vulnerable to unauthorized disclosure.

140. Defendant knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would result if Plaintiffs' and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach.

141. The risk of improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' Private Information from that risk left the Private Information in a dangerous condition.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

142. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Private Information was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

K. Plaintiffs' Experiences

Plaintiff Diana Saiki

143. Plaintiff Saiki is a patient of IU Health, an Indiana University Health Affiliated Covered Entity. She provided her personal and health information to IU Health in order to receive medical services. MCG provides patient care guidelines to health care providers and health plans, including IU Health. MCG received Plaintiff's personal and health information in connection with providing those services to IU Health.

144. Plaintiff Saiki received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Saiki's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

145. In response to receiving the letter, Plaintiff Saiki has spent at least two hours checking credit reports, financial accounts, and ordering a credit report.

146. Plaintiff Saiki paid for her medical services and medical insurance with the expectation that her medical providers, medical insurance company, and its service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

147. Plaintiff Saiki suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

148. Plaintiff Saiki also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

149. Plaintiff Saiki suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff Saiki has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Leo Thorbecke

150. Plaintiff Leo Thorbecke is a patient of IU Health, an Indiana University Health Affiliated Covered Entity. Mr. Thorbecke provided his personal and health information to IU Health in order to receive healthcare services. MCG provides patient care guidelines to Indiana University Health Affiliated Covered Entities, and received Mr. Thorbecke's personal and health information in connection with providing those services.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

151. Plaintiff Thorbecke received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained his personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

152. Since being notified of the Data Breach, Mr. Thorbecke has spent approximately eight hours attempting to mitigate the impact of his stolen personal and medical information.

153. Plaintiff Thorbecke paid for medical services with the expectation that his healthcare provider and its service providers, including MCG, would keep his information secure and inaccessible from unauthorized parties.

154. Plaintiff Thorbecke suffers stress and frustration as a result of the Data Breach and from the loss of his privacy.

155. Plaintiff Thorbecke also suffered injury in the form of damage to and diminution in the value of his confidential personal information—a form of property that Plaintiff Thorbecke entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

156. Plaintiff Thorbecke suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from his personal information—especially his Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff Thorbecke has a continuing interest in ensuring that his personal information is protected and safeguarded from future breaches.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff Kenneth Hensley's minor child R.H.

157. Plaintiff Hensley received a letter from MCG Health dated June 10, 2022, advising that his minor child R.H.'s information was acquired by cybercriminals in the Data Breach. The letter advised that the information of R.H.'s that has been compromised in the Data Breach includes some or all of the following PII and PHI: name, Social Security number, date of birth, medical codes, postal address, telephone numbers, email addresses, and gender.

158. As required in order to obtain medical services, Plaintiff Hensley provided R.H.'s highly sensitive personal and health information, including the Private Information that was compromised in the Data Breach.

159. Because of Defendant's negligence and failure to properly secure the Private Information in its possession, which negligence and failure led to the Data Breach, R.H.'s Private Information has been obtained by cybercriminals.

160. Plaintiff Hensley has received alerts through Experian that the phone number associated with R.H. was found on the dark web on February 4, 2022 and June 17, 2022.

161. R.H. is now under an imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of R.H.'s life. The imminent risk of identity theft and fraud R.H. now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendant in its failure to implement adequate data security protocols, which negligence led to the Data Breach.

162. As a result of the Data Breach, Plaintiff Hensley has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for R.H., including investigating the Data

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Breach, investigating how best to ensure that R.H. is protected from identity theft, and securing identity theft protection services for R.H.

163. As a direct and proximate result of the Data Breach, Plaintiff Hensley will need to pay for identity theft protection for the rest of R.H.'s lifetime.

164. Plaintiff Hensley suffers stress and anxiety as a result of the Data Breach and from the loss of his minor child's privacy

165. R.H. has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of R.H.'s Private Information that was entrusted to Defendant for the sole purpose of obtaining medical services necessary for R.H.'s health and well-being, with the understanding that Defendant would safeguard this information against unauthorized disclosure. Additionally, R.H.'s Private Information is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendant and is subject to future wrongful disclosures and/or security breaches so long as Defendant fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Plaintiff Michael Price

166. Plaintiff Price was a patient of IU Health, an Indiana University Health Affiliated Covered Entity. Plaintiff Price provided his personal and health information to IU Health in order to receive medical services. MCG provides patient care guidelines to IU Health and received Plaintiff Price's personal and health information in connection with providing those services.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

167. Plaintiff Price received a letter in June 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Price's Private Information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

168. Plaintiff Price paid for medical services with the expectation that his healthcare provider and its service providers, like MCG, would keep his information secure and inaccessible from unauthorized parties.

169. Plaintiff Price suffers stress and anxiety as a result of the Data Breach and from the loss of his privacy.

170. Plaintiff Price also suffered injury in the form of damage to and diminution in the value of his confidential personal information—a form of property that Plaintiff Price entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

171. Plaintiff Price estimates that he spent approximately 10 hours researching the Data Breach, scrutinizing his accounts, examining his records and credit scores and otherwise addressing the Data Breach.

172. Plaintiff Price suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from his personal information—especially his Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff Price has a continuing interest in ensuring that his personal information is protected and safeguarded from future breaches.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff Linda Crawford

173. Plaintiff Crawford is a member of Medicare Advantage through Aetna and obtained medical care through Newman Regional Health in Burlington, KS. Plaintiff Crawford provided her personal and health information to Aetna and Newman Regional Health in order to receive health insurance and medical care. MCG provides patient care guidelines to Aetna and Newman Regional Health, and received Plaintiff Crawford's personal and health information in connection with providing those services.

174. Plaintiff Crawford received a letter from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Crawford's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

175. In or around late 2021 or early 2022, Plaintiff Crawford experienced identity theft and credit fraud when loans were opened in her name. Plaintiff Crawford also received a fraud alert on August 30, 2022. As a result, Plaintiff Crawford's credit rating fell 80 points, and Plaintiff Crawford purchased credit monitoring. Plaintiff Crawford has spent at least 20 hours disputing the fraudulent accounts and reviewing account statements, credit reports, and monitoring services since the Data Breach.

176. Plaintiff Crawford had not experienced any instances of identity theft, fraud, or credit fraud before February 2020 and has not received notification from any other company that her personal information may have been exposed.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

177. Plaintiff Crawford paid for medical services and health insurance with the expectation that Aetna and Newman Regional Health and their service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

178. Plaintiff Crawford suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

179. Plaintiff Crawford also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

180. Plaintiff Crawford suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Kelly Batt

181. Plaintiff Batt is a patient of Centinela Hospital Medical Center. Plaintiff Batt provided her personal and health information to Centinela Hospital Medical Center in order to receive medical services. MCG provides patient care guidelines to Centinela Hospital Medical Center, and received Plaintiff Batt's personal and health information in connection with providing those services.

182. Plaintiff Batt received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Batt's personal information from data stored on MCG's systems. The compromised information includes names,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

183. Plaintiff Batt obtained medical services with the expectation that Centinela Hospital Medical Center and its service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

184. Plaintiff Batt suffers stress, anxiety, and frustration as a result of the Data Breach and from the loss of her privacy.

185. Plaintiff Batt has already expended time to address the Data Breach and to attempt to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach and options for how to protect her interests in response to the Data Breach.

186. Plaintiff Batt also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Batt entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

187. Plaintiff Batt suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Shelley Taylor

188. Plaintiff Shelley Taylor is a patient of Catholic Health Initiative. Patient Shelley Taylor provided her personal and health information to Catholic Health Initiative in order to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

receive medical services. MCG provides patient care guidelines to Catholic Health Initiative and received Plaintiff Shelley Taylor's personal and health information in connection with providing those services.

189. Plaintiff Shelley Taylor received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Shelley Taylor's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

190. In response to the Data Breach, Plaintiff Shelley Taylor spent approximately 15 hours searching the Internet for information about the Data Breach, signing up for credit monitoring, searching for credit monitoring services, changing passwords, and checking financial accounts for potential fraud.

191. Plaintiff Shelley Taylor paid for medical services with the expectation that Catholic Health Initiative and its service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

192. Plaintiff Shelley Taylor suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

193. Plaintiff Shelley Taylor also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Shelley Taylor entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

194. Plaintiff Shelley Taylor suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Jay Taylor

195. Plaintiff Jay Taylor is a patient of Catholic Health Initiative. Patient Jay Taylor provided his personal and health information to Catholic Health Initiative in order to receive medical services. MCG provides patient care guidelines to Catholic Health Initiative and received Plaintiff's personal and health information in connection with providing those services.

196. Plaintiff Taylor received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

197. In response to the Data Breach, Plaintiff Taylor spent approximately 12 hours searching the Internet for information about the Data Breach, attempting to get on the Experian website to sign up for credit monitoring, searching for credit monitoring services, changing passwords, and checking financial accounts for potential fraud.

198. Plaintiff Taylor paid for medical services with the expectation that Catholic Health Initiative and its service providers, like MCG, would keep his information secure and inaccessible from unauthorized parties.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

199. Plaintiff Taylor suffers stress and anxiety as a result of the Data Breach and from the loss of his privacy.

200. Plaintiff Taylor also suffered injury in the form of damage to and diminution in the value of his confidential personal information—a form of property that Plaintiff entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

201. Plaintiff Taylor suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from his personal information—especially his Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff has a continuing interest in ensuring that his personal information is protected and safeguarded from future breaches.

Plaintiff Gaye Ictech

202. Upon information and belief, Plaintiff Ictech is a patient of healthcare provider, health insurance company, or health plan that utilizes MCG's services. Plaintiff Ictech provided her personal and health information to the MCG affiliated healthcare provider, health insurance company, or health plan in order to receive medical services and/or health insurance. MCG received Plaintiff Ictech's personal and health information in connection with providing its services to one of more of Plaintiff Ictech's health providers, health plan, or health insurance company.

203. Plaintiff Ictech received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Ictech's personal information from data stored on MCG's systems. The compromised information includes names,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

204. In response to the letter, Plaintiff Ictech has spent approximately twenty (20) hours addressing the Data Breach, signing up for the offered credit monitoring service, and searching for fraudulent activity on financial accounts. Moreover, Plaintiff Ictech experienced an increase in targeted and suspicious spam calls that caused additional loss of time and annoyance.

205. Furthermore, in March, 2021 and March 2022, Plaintiff Ictech experienced multiple fraudulent charges on her debit card, which she then had to cancel in response to the fraud. This card was provided to and used to pay for health services and health insurance premiums prior to the Data Breach.

206. Plaintiff Ictech paid for medical services and health insurance with the expectation that healthcare provider and insurer and its service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

207. Plaintiff Ictech suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

208. Plaintiff Ictech also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

209. Plaintiff Ictech suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

parties. Plaintiff Ictech has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Cynthia Strecker

210. Plaintiff Strecker is a patient of healthcare provider, health insurance company, or health plan that utilizes MCG's services. Plaintiff Strecker provided her personal and health information to the MCG affiliated healthcare provider, health insurance company, or health in order to receive medical services and/or health insurance. MCG received Plaintiff Strecker's personal and health information in connection with providing its services to one of more of Plaintiff Strecker's health providers, health plan, or health insurance company.

211. Plaintiff Strecker received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Strecker's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

212. In response to receiving the letter from MCG, Plaintiff Strecker spent approximately five hours of time researching the Data Breach, and reviewing financial accounts.

213. Plaintiff Strecker paid for medical services and health insurance with the expectation that healthcare provider and medical insurer and their respective service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

214. Plaintiff Strecker suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

215. Plaintiff Strecker also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Strecker entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

216. Plaintiff Strecker suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Candace Daugherty

217. Plaintiff Daugherty is a patient of Southern Surgery Center and Plaintiff's health insurance provider is Blue Cross Blue Shield. Plaintiff Daugherty provided her personal and health information to Southern Surgery Center and Blue Cross Blue Shield in order to receive medical services and health insurance. MCG provides patient care guidelines to Southern Surgery Center and Blue Cross Blue Shield, and received Plaintiff Daugherty's personal and health information in connection with providing those services.

218. Plaintiff Daugherty received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Daugherty's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

219. Since the Data Breach, Plaintiff Daugherty experienced attempted identity theft and credit fraud when hackers attempted to log into her bank account and credit union account.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff Daugherty found two unauthorized charges on her bank account. An unauthorized person also attempted to create an eBay account under Plaintiff Daugherty's name multiple times. Plaintiff Daugherty must constantly reset her email password because of failed log in attempts from unknown individuals.

220. Plaintiff Daugherty paid for medical services and health insurance with the expectation that they and their service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

221. Plaintiff Daugherty suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

222. Plaintiff Daugherty also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Daugherty entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

223. Plaintiff Daugherty suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff Daugherty has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Linda Booth

224. Plaintiff Booth is a member of Christus Health Plan. Plaintiff Booth provided her personal and health information to Christus Health Plan in order to receive health insurance.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

MCG provides patient care guidelines to Christus Health Plan and received Plaintiff Booth's personal and health information in connection with providing those services.

225. Plaintiff Booth received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Booth's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

226. Plaintiff Booth paid for health insurance with the expectation that Christus Health Plan and its service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

227. As a result of the Data Breach, Plaintiff Booth upgraded her Norton identity theft protection subscription.

228. Plaintiff Booth estimates she spent nearly 40 hours investigating and otherwise addressing the Data Breach, including researching the breach, placing freezes on her credit report, contacting Social Security to lock her social security number, and reviewing her credit reports thoroughly.

229. Plaintiff Booth suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy and she worries about criminals having access to her medical information.

230. Plaintiff Booth also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Booth entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

231. Plaintiff Booth suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Blanca Garcia

232. Plaintiff Garcia was a patient of El Paso Specialty Hospital ("El Paso"). Plaintiff Garcia provided her personal and health information to in order to receive medical services. MCG provides patient care guidelines to El Paso and received Plaintiff Garcia's personal and health information in connection with providing those services.

233. Plaintiff Garcia received a letter dated June 3rd, 2022 from Surgery Partners, a former affiliate of El Paso, concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Garcia's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

234. In response to receiving the letter, Plaintiff Garcia has spent approximately four to five hours reviewing accounts and looking for fraudulent activity.

235. Furthermore, Since February, 2020, she has noticed unauthorized charges on her credit cards. She spent additional time addressing the charges and cancelling her cards.

236. Plaintiff Garcia paid for medical services with El Paso with the expectation that her healthcare provider and its service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

237. Plaintiff Garcia suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

238. Plaintiff Garcia also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

239. Plaintiff Garcia suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff Garcia has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Marjorita Dean

240. Plaintiff Dean is a patient of Sheltering Arms Hospital Foundation, Inc. ("Sheltering Arms"), operating under OhioHealth O'Bleness Memorial Hospital. Plaintiff Dean provided her personal and health information to Sheltering Arms in order to receive medical services. MCG provides patient care guidelines to Sheltering Arms and received Plaintiff Dean's personal and health information in connection with providing those services.

241. Plaintiff Dean received a letter on or around June 16, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Dean's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

242. Plaintiff Dean paid for medical services with the expectation that her healthcare provider and its service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

243. Plaintiff Dean suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy, particularly stress about how the exfiltration of her private information could impact her family business.

244. Plaintiff Dean also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Dean entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

245. Plaintiff Dean estimates that she spent approximately 5 hours researching the Data Breach, checking her accounts, scrutinizing her records and credit scores, signing up for identity theft protection through MCG and otherwise addressing the Data Breach.

246. Plaintiff Dean suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third parties. Plaintiff Dean has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Julie Mack

247. Plaintiff Mack is a patient of Dallas Medical Center. Patient provided her personal and health information to Dallas Medical Center in order to receive medical services. MCG provides patient care guidelines to Dallas Medical Center and received Plaintiff Mack's personal and health information in connection with providing those services.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

248. Plaintiff Mack received a letter dated June 20, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Mack's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

249. On August 23, 2022, Plaintiff Mack received an alert through McAfee that her email address was found on the dark web.

250. Plaintiff Mack paid for medical services with the expectation that healthcare provider and its service providers, like MCG, would keep her information secure and inaccessible from unauthorized parties.

251. Plaintiff Mack suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

252. Plaintiff Mack also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Mack entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

253. Plaintiff Mack estimates that she spent approximately 30 hours researching the Data Breach, looking over her accounts, scrutinizing her records and credit scores and otherwise addressing the Data Breach.

254. Plaintiff Mack suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number and medical information—being placed in the hands of unauthorized third

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

parties. Plaintiff Mack has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Joanne Mullins

255. Plaintiff Mullins is a patient of Catholic Health Initiatives ("CHI"). Ms. Mullins provided her personal and health information to CHI in order to receive medical services. MCG provides patient care guidelines to CHI and its Affiliates, and received Plaintiff Mullin's personal and protected health information in connection with providing those services.

256. Plaintiff Mullins received a letter dated June 10, 2022 from MCG concerning the Data Breach. The letter stated that an unauthorized party obtained Plaintiff Mullin's personal information from data stored on MCG's systems. The compromised information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

257. On September 23, 2021, an unauthorized actor used Plaintiff Mullins' email address and PayPal account to charge $375 for a denim jacket from a vendor called "Axel Arigato AB." Plaintiff Mullins did not make or authorize the charges

258. Since receiving the June 10, 2022 letter from MCG concerning the Data Breach, Ms. Mullins has spent 3-5 hours attempting to mitigate the impact of the Data Breach.

259. Plaintiff Mullins paid for medical services with the expectation that her healthcare provider and its service providers, including MCG, would keep her information secure and inaccessible from unauthorized parties.

260. Plaintiff Mullins suffers stress and anxiety as a result of the Data Breach and from the loss of her privacy.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

261. Plaintiff Mullins also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Mullins entrusted to MCG, which was compromised as a result of the Data Breach it failed to prevent.

262. Plaintiff Mullins suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her Social Security number, email address and medical information—being placed in the hands of unauthorized third parties. Plaintiff Mullins has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

263. Plaintiffs bring this lawsuit as a class action on behalf of themselves and on behalf of all other persons similarly situated, pursuant to Federal Rules of Civil Procedure 23(a) and (b)(2), (b)(3), and/or (c)(4). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements.

264. The proposed Class is defined as:

> All United States residents whose Private Information was accessed or acquired during the Data Breach (the "Nationwide Class" or "Class").

265. Plaintiffs also seek to represent the following state subclasses defined as:

> All Kansas residents whose Private Information was accessed or acquired during the Data Breach (the "Kansas Subclass");
>
> All Louisiana residents whose Private Information was accessed or acquired during the Data Breach (the "Louisiana Subclass");

266. The Nationwide Class and the state Subclasses are referred to collectively as the Class. Excluded from the Class are Defendant, any entity in which Defendant has a controlling

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

267. Plaintiffs reserve the right to modify, change, or expand the Class and Subclass definitions, including by proposing additional subclasses, based on discovery and further investigation.

268. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on Defendant's disclosures to State Attorneys general, the Class consists of approximately 1,100,000 individuals whose sensitive data was compromised in Data Breach.

269. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class Member because Plaintiffs and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Defendant.

270. Adequacy: Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class they seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

271. Superiority: A class action is superior to other alternatives for the fair and efficient adjudication of this controversy. The injury suffered by each individual class member is

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

272. Commonality and Predominance: Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out below predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

273. There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. Whether Defendant's computer systems and data security practices used to protect Plaintiffs' and Class Members' Private Information violated the FTC Act and/or HIPAA, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiffs and Class Members to adequately protect their Private Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to a data breach or disclosure;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties regarding Plaintiffs and Class Members to use reasonable care in protecting their Private Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

i. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

j. Whether Plaintiffs and Class Members are entitled to recover damages, equitable relief, and other relief;

k. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

l. Whether Defendant's actions and inactions alleged herein constitute gross negligence; and

m. Whether Plaintiffs and Class Members are entitled to statutory damages.

274. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

275. Defendant has acted or refused to act on grounds generally applicable to the entire Class, making injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Class)

276. Plaintiffs incorporate by reference the foregoing allegations of fact as if fully set forth herein.

277. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of the regular course of its business operations. Plaintiffs and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

278. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

279. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

280. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

281. Additionally, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until June 10, 2022, despite knowing by

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

March 25, 2022 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

282. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

283. Defendant's conduct, as alleged herein, allowed it to gain a competitive advantage over companies offering the same or similar services because, rather than properly fund data security protocols, as required by HIPAA and industry standards, Defendant diverted that money towards its own profit. Defendant's conduct, and the unfair advantage realized thereby, creates a race to the bottom by encouraging companies to divert funds intended for data security towards profits in order to remain competitive. The end effect is that both consumers and the marketplace in general are harmed through the widespread adoption of substandard data security practices and the concomitantly increased risk of cyberattacks (which disrupt the provision of medical services) and fraud and identity theft (which disrupt the lives of victims and impose a burden on the state to investigate and prevent criminal activity).

284. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

285. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

286. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

287. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein. Defendant's failure to use reasonable data security measures allows it to gain an unfair advantage over its competitors, realize greater profits, and harms both Defendant's immediate competition and the marketplace in general.

288. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

289. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

290. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

291. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Private Information that was in Defendant' possession. As a result of Defendant's assumption of control over their Private Information, Plaintiffs and Class Members were totally unable to protect themselves against the risk of a cyberattack and were completely dependent on Defendant to ensure that their Private Information was secured against a targeted data breach, as occurred here.

292. By collecting and taking custody of Plaintiffs and Class Members' Private Information with full awareness of both the likelihood of a cyberattack targeted to acquire that information and the severe consequences that would result to Plaintiffs and Class Members if the confidentiality of the Private Information was breached, Defendant assumed a special relationship that required it to guard against the foreseeable conduct of a criminal third party. If Defendant had not intervened by taking charge of Plaintiffs' and Class Member's Private Information, no harm would have resulted to Plaintiffs and Class Members as a result of the Data Breach.

293. By taking charge of and assuming custody over the Private Information to which it was entrusted, Defendant was required to supervise the integrity of its data security systems and the information stored therein. Defendant was fully aware of the identity of each individual for whom it custodied Private Information and was further aware that it was in an exclusive position to guard against the harm that would result to those individuals if it failed to guard against a cyberattack.

294. Defendant was in a special relationship with Plaintiffs and Class Members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiffs and Class Members by ensuring that their personal information would remain

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiffs' and Class Members' personal and medical information. Plaintiffs and Class Members had no ability to influence Defendant's data security policies or verify the integrity of those policies and practices. The harm to Plaintiffs and Class members from its exposure was highly foreseeable to Defendant.

295. As a result of the special relationship, Defendant owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

296. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

297. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs and the Class include:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiffs and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

298. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

299. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and Class Members' Private Information;

f. Failing to mitigate the harm caused to Plaintiffs and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiffs and Class Members of the Data Breach that affected their Private Information.

300. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

301. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

302. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

303. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

304. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

305. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

306. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

307. Plaintiffs and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

COUNT II
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
RCW 19.86.010, *et seq.*,
(On behalf of Plaintiffs and the Class)

308. Plaintiffs incorporate by reference the foregoing allegations of fact as if fully set forth herein.

309. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

310. Defendant is a "person" as described in RWC 19.86.010(1).

311. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

312. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

313. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' Private Information, and violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

314. Defendant also violated the CPA by failing to timely notify and concealing from Plaintiffs and Class Members information regarding the unauthorized release and disclosure of their Private Information. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information, medical information, and identities.

315. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

316. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

317. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their Private Information; (5) deprivation of the value of their Private Information, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

318. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

319. Plaintiffs, on behalf of themselves and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiffs, on behalf of themselves and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.

COUNT III
VIOLATION OF THE KANSAS DATA BREACH REQUIREMENTS ACT
Kan. Stat. Ann. §§ 50-7a02(a), *et seq.*
(On behalf of Plaintiff Crawford and the Kansas Subclass)

320. Plaintiff Crawford re-alleges and incorporates by reference all preceding factual allegations as if fully set forth herein.

321. Plaintiff Crawford ("Plaintiff" for the purposes of this Count) brings this Count on her own behalf and on behalf of the Kansas Subclass.

322. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. §§ 50-7a02(a).

323. Plaintiff's and Kansas Subclass members' PII constitute Personal Information under Kan. Stat. Ann. §§ 50-7a02(a).

324. Kansas law requires Defendant to notify, in the most expedient time possible and without unreasonable delay, Plaintiff and Kansas Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

325. Because Defendant was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, it was required to disclose the data breach in a timely and accurate fashion under Kan. Stat. Ann. § 50- 7a02(a).

326. By failing to disclose the data breach in a timely and accurate manner, Defendant violated Kan. Stat. Ann. § 50-7a02(a).

327. As a direct and proximate result of Defendant's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages, as described above.

328. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT IV
VIOLATION OF THE LOUISIANA DATABASE SECURITY BREACH NOTIFICATION LAW
La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.*
(On behalf of Plaintiff Ictech and the Louisiana Subclass)

329. Plaintiff Ictech re-alleges and incorporates by reference all preceding factual allegations as if fully set forth herein.

330. Plaintiff Ictech ("Plaintiff" for the purposes of this Count) bring this Count on her own behalf and on behalf of the Louisiana Subclass.

331. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

332. Plaintiff's and Louisiana Subclass members' PII includes Personal Information as covered under La. Rev. Stat. Ann. § 51:3074(C).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

333. Under La. Rev. Stat. Ann. § 51:3074(C), Defendant was required accurately notify, in the most expedient time possible and without unreasonable delay, Plaintiff and Louisiana Subclass members if it became aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information.

334. Because Defendant was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiff's and Louisiana Subclass members' Personal Information, it was required to disclose the data breach in a timely and accurate fashion under La. Rev. Stat. Ann. § 51:3074(C).

335. By failing to disclose the data breach in a timely and accurate manner, Defendant violated La. Rev. Stat. Ann. § 51:3074(C)).

336. As a direct and proximate result of Defendant's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages as described above.

337. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class and Subclasses pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23 on behalf of the Class and Subclasses defined herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class and Subclasses;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

b. A judgment in favor of Plaintiffs and the Class and Subclasses awarding them appropriate monetary relief, including actual damages, treble damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and Subclasses as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class and Subclasses awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: July 14, 2023

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Jason T. Dennett*
Jason T. Dennett, WSBA #30686
s/ Rebecca L. Solomon
Rebecca L. Solomon, WSBA #51520
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
Tel: (206) 682-5600/Fax: (206) 682-2992
jdennett@tousley.com
rsolomon@tousley.com

Gary M. Klinger**
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100

Chicago, IL 60606
Telephone: (202) 429-2290
gklinger@milberg.com

Bryan L. Bleichner**
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300/Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
Beth E. Terrell (WSBA #26759)
Jennifer Rust Murray (WSBA #36983)
TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, WA 98103-8869
Telephone: 206-816-6603
Facsimile: 206-319-5450
bterrell@terrellmarshall.com
jmurray@terrellmarshall.com

Adam E. Polk (CA State Bar No. 273000)**
Simon Grille (CA State Bar No. 294914)**
Jessica Cook (CA State Bar No. 339009)**
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
apolk@girardsharp.com
sgrille@girardsharp.com
jcook@girardsharp.com

Joseph M. Lyon **
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
Email: jlyon@thelyonfirm.com

William B. Federman**
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120

Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
-and-
212 W. Spring Valley Road
Richardson, Texas 75081

A. Brooke Murphy**
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Benjamin F. Johns **
Samantha E. Holbrook**
Chimicles Schwartz Kriner
& Donaldson-Smith LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Tel: (610) 642-8500
Fax: (610) 649-3633
bfj@chimicles.com
seh@chimicles.com

Terence R. Coates**
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

M. ANDERSON BERRY*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com

Jeffrey S. Goldenberg**

GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
(513) 345-8291
jgoldenberg@gs-legal.com

Charles E. Schaffer**
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
(215) 592-1500
cschaffer@lfsblaw.com

Samuel J. Strauss (WSBA 46971)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com

Jonathan M. Lebe (State Bar No. 284605)*
Jon@lebelaw.com
Yuri A. Chornobil (State Bar No. 331905)*
Yuri@lebelaw.com
Lebe Law, APLC
777 S. Alameda Street, Second Floor
Los Angeles, CA 90021
Telephone: (213) 444-1973

Gary E. Mason**
Danielle Perry*
Mason LLP
5101 Wisconsin Ave., NW, Ste 305
Washington, DC 20016
T: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com

**pro hac vice request* forthcoming
***Admitted *pro hac vice*

Counsel for Plaintiffs and the Class

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992